

REMARKS

The present claim amendments and cancellations are submitted pursuant to the examiner's comments in a final office action letter dated August 3, 2007. These amendments and cancellations are entered in order to place the claims into condition for allowance in view of said examiner's letter. However, applicants are not conceding in this application that other claims as originally filed or amended in the prosecution of this case are not patentable over the prior art of record, and applicants reserve the right to pursue any of the originally submitted claims 1-35, as well as other claims, in one or more continuations and/or divisional patent applications.

Moreover, of the original claims 1-35, those not cancelled are presently amended or have been previously amended by applicants' filing on May 30, 2007. Contrary to the examiner's statement in his letter of August 3, 2007, applicants have not failed to "seasonably challenge" the examiner's assertions. Instead, those assertions were rendered moot by said claim amendments and, as the issue was not ripe for traversal, applicants had and have no obligation to traverse said assertions. Applicants expressly reserve the right to address and contravene the examiner's assertions if they become ripe.

Claim Rejections - 35 USC § 103

Claims 1, 2, 8-12, 16-22, 25-26, 30, 34 and 35 stand rejected under 35 USC § 103(a) as being unpatentable over Shanklin et al. (U.S. Pat. No. 6487666) in view of Tarquini et al. (U.S. Pat. Publication No. 2003/0101353). In rejecting claims under 35 U.S.C. §103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1986). In so doing, the examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the

art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir.1984)..

The examiner has failed to show that Shanklin et al. in view of Tarquini et al. teach **all** of the limitations specifically claimed in independent method claim 1 as previously amended on May 30, 2007. More specifically, claim 1 claims a method for monitoring network communications for a specifically defined predefined sequential triplet of TCP/IP protocol set packets, the triplet (1) an initial SYN packet *originating from a source address*, (2) a next sequential SYN/ACK packet *issuing from a target device address* in response to the SYN packet, and (3) a last sequential RST packet *originating from the source address* in response to the SYN/ACK packet, wherein an unauthorized scanning alert is issued **if each** of the predefined sequence of packets are relevant to **the source address**.

In his letter of August 3, 2007 at item 4, page 3, the examiner expressly acknowledges that Shanklin et al does not teach this “source address” claim limitation subject matter, yet fails to cite how Tarquini et al. supplies the requisite missing teachings. The examiner’s rejection of claim 1 is thus unsupported at law and not believed to be well-taken, and the examiner is respectfully requested to remove his rejection of claim 1 under 35 USC § 103(a) over Shanklin et al. in view of Tarquini et al.

Moreover, Tarquini et al. does not supply the missing teachings. The examiner’s only citation to Tarquini et al. (at paragraph 44) discusses instead NMAP probing utilities that use TCP SYN scans to find open ports. There is no teaching as to how to recognize and issue an attack alert through observation of a SYN packet *originating source address*, and one skilled in the art would not arrive at the claimed invention through Shanklin et al. in view of Tarquini et al. Instead, Shanklin et al. in view of Tarquini et al. teaches intrusion detection through divergent methodology that teaches away from applicants’ claimed invention. Packet origin addresses are irrelevant to Shanklin et al. in view of Tarquini et al.

More particularly, In the case of In re Wesslau, 353 F. 2d 238 (CCPA 1965), the court held:

“It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.” (emphasis original)

Similarly, in Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc. et al, 796 F.2d 443, 230 U.S.P.Q 416 (Fed. Cir. 1986), the court held: “The ... court failed to consider the Caddell reference in its entirety and thereby ignored the portions of the reference that argued against obviousness. (citations)”

Thus, it is clear that when a reference is used in a §103 citation, the entire reference must be used. One may not pick and choose from a given reference only those portions which support an espoused position, and ignore those portions which do not support that position, which is clearly the case here with respect to Shanklin et al., which teaches detection of attack “signatures” through evidence of packet types, frequencies and counts over time periods, but not by identifying an attack signature through source address, or any other address indicia. Instead, the examiner’s own citation to Shanklin et al. (Column 6, lines 14-20) clearly states that an attack signature (a “SYN flood”) is indicated by a number of SYN packets “for any host...In other words, the number of SYN packets ...within a certain time period, Time, is counted” (emphasis added). By “any host” Shanklin et al. clearly means that identifying and considering the source address is irrelevant, as established by material immediately before the present citation, at Column 6, lines 5-7, “...the SYN Flood attack is characterized by an influx of SYN packets ... *from random IP addresses* within a short time period” (emphasis added). Thus, one skilled in the art would learn from Shanklin et al. to *ignore* a source address, as such observation offers *no* advantage in preventing attacks through techniques and methods taught by Shanklin et al. This is clearly and unambiguously teaching away from applicants’ claimed invention.

Additionally, Tarquini et al. does not supply the missing teachings. As confirmed by a text search of Tarquini et al., no relevant teachings as to source address identification are present within the entire reference, nor would such teaching be implied through the

examiner's citation or any other portion. Moreover, regardless of the examiner's assertions with regard to "creating an expression in order to detect the TCP SYN scan," the remainder of page 3 of his letter of August 3, 2007 does not assert or otherwise establish that Shanklin et al. in view of Tarquini et al. teaches the specific "source address" limitations claimed by claim 1. (The examiner's position thus traversed, applicants need not address these examiner's assertions as to what would be obvious to one skilled in the art at this time, and applicants do not admit that said assertions signify admitted prior art of record in the course of prosecution of this or any related case.)

Claim 2 has been cancelled and its rejection (and the examiner's related assertions) rendered moot. Furthermore, applicants do not admit that the limitations of claim 2 are disclosed by Shanklin et al., but instead expressly reserve the right to pursue this subject matter in further divisional and continuation applications.

Claim 8 is indirectly dependent upon claim 1 and incorporates all of its limitations as well as those of amended claim 4. It is thus believed allowable over Shanklin et al. in view of Tarquini et al. under 35 USC § 103(a) for the reasons established above with respect to claim 1, and further as established below with respect to amended claim 4.

Claims 9 and 10 are indirectly dependent upon claim 1 and incorporate all of its limitations as well as those of amended claim 4. They are thus believed allowable over Shanklin et al. in view of Tarquini et al. under 35 USC § 103(a) for the reasons established above with respect to claim 1, and further as established below with respect to amended claim 4. Moreover, amended claims 9 and 10 claim additional specific limitations not taught by Shanklin et al. in view of Tarquini et al.; blocking future packets comprising the *source address*, the target device address and a target device port address, and rate-limiting flows of packets comprising the *source address*, respectively. Neither of these specific limitations is taught by Shanklin et al. in view of Tarquini et al., and thus amended claims 9 and 10 are believed allowable for these additional reasons. And since the examiner's assertions with regard to "Official Notice" in his item number 7 on page 4 of the August 3, 2007 Office action do not establish that Shanklin et al. in view of Tarquini et al. teach the limitations claimed by amended claims 9 and 10, applicants need not address nor traverse the examiner's assertion at this time, as the issue is moot. Furthermore, applicants

do not admit that said assertion signifies admitted prior art of record in the course of prosecution of this or any related case.

Claims 25 and 30 are independent method claims incorporating limitations analogous to those discussed with respect to claim 1, and are thus believed to be allowable over Shanklin et al. in view of Tarquini et al. for the reasons established above. And claims 26 and 34 are dependent upon claims 25 and 30, respectively, and thus each incorporate all of their respective limitations and are also believed allowable over Shanklin et al. in view of Tarquini et al. under 35 USC § 103(a).

Claims 3 and 4 stand rejected under 35 USC § 103(a) as being unpatentable over Shanklin et al. in view of Tarquini et al. in view of Etheridge et al. (US Patent Publication No. 2004/0054925). However, the examiner cites to Etheridge et al. only for teachings with respect to histogram-related limitation teachings in claims 3 and 4. Claims 3 and 4 depend directly and indirectly, respectively, upon claim 1 and thus incorporate all of its limitations and are thus believed to be allowable over Shanklin et al. in view of Tarquini et al. in view of Etheridge et al. for the reasons established above.

Moreover, the examiner errs in asserting that Etheridge et al. at paragraph 84 offers any relevant teachings as to tracking source addresses in view of Shanklin et al. As established above with respect to claim 1, Shanklin et al. teaches away from identifying an attack signature through observing a source address, or any other address indicia, instead observing that the source addresses may be *random*. Thus, the examiner's position is clearly in error. One skilled in the art learns from Shanklin et al. that attacker addresses are *random*, and thus tracking said addresses to identify future attacks would be pointless. It is impossible and illogical to state that one skilled in the art would then modify Shanklin et al. by "rationally assuming that source address must be somewhat correlated to the current count of SYN packets." Thus, Etheridge does not supply the missing teachings, and amended claims 3 and 4 are believed allowable under 35 USC § 103(a) over Shanklin et al. in view of Tarquini et al. in view of Etheridge et al.

New Claims

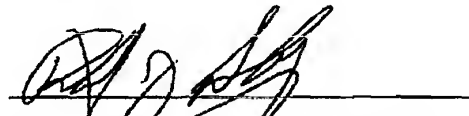
New claims 36-51 are all directly or indirectly dependent upon claims allowable as established above, incorporating their limitations, as well as claiming additional limitations. They are all, therefore, believed to be allowable, including for the reasons established above.

Conclusion

The examiner's rejection of claims 1, 25, 26 and 30 in his letter of August 3, 2007 is not believed to be supported or well taken as established above, and withdrawal of said rejection is respectfully requested. And amended claims 3, 4, 8-10 and 34 and new claims 36-51 are all believed to be allowable over the prior art of record.

Respectfully submitted,

Date: September 28, 2007



Patrick J. Daugherty, Reg. No. 41,697

CUSTOMER NO. 26675